(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11306088 A**

(43) Date of publication of application: **05 . 11 . 99**

(51) Int. Cl **G06F 12/14**
G06K 17/00
G06K 19/073
G09C 1/00
H04L 9/32

(21) Application number: **10117394**

(22) Date of filing: **27 . 04 . 98**

(71) Applicant: **TOPPAN PRINTING CO LTD**

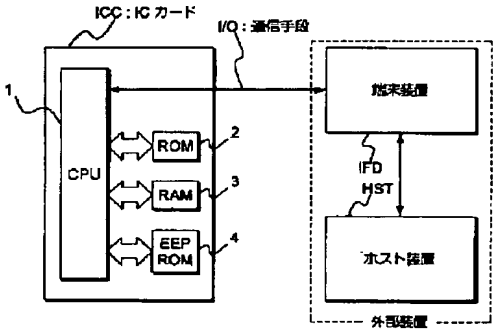
(72) Inventor: **YURA AKIYUKI**
MATSUMURA SHUICHI
FUNADOGAWA NORIO

(54) **IC CARD AND IC CARD SYSTEM**

(57) Abstract:

PROBLEM TO BE SOLVED: To provide an IC card and IC card system capable of preventing IC card data from being illegally obtained.

SOLUTION: A CPU 1 unidirectionally adds or subtracts a specified value to/from additional data stored in an EEPROM 4 each time a piece of instruction data is received from a terminal device IFD. Moreover, the CPU 1 adds the added or subtracted additional data to the instruction data, allows a specific secret key to encipher the instruction data with these addition data added, and makes them data which are transmitted and received on a communication means.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－306088

(43)公開日　平成11年(1999)11月５日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	12/14	３２０	Ｇ０６Ｆ	12/14	３２０Ａ
Ｇ０６Ｋ	17/00		Ｇ０６Ｋ	17/00	Ｅ
	19/073		Ｇ０９Ｃ	1/00	６６０Ａ
Ｇ０９Ｃ	1/00	６６０	Ｇ０６Ｋ	19/00	Ｐ
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７５Ａ

審査請求　未請求　請求項の数10　ＯＬ　（全８頁）

(21)出願番号　特願平10－117394

(22)出願日　平成10年(1998)４月27日

(71)出願人　000003193
凸版印刷株式会社
東京都台東区台東１丁目５番１号

(72)発明者　由良　彰之
東京都台東区台東１丁目５番１号　凸版印刷株式会社内

(72)発明者　松村　秀一
東京都台東区台東１丁目５番１号　凸版印刷株式会社内

(72)発明者　船渡川　紀夫
東京都台東区台東１丁目５番１号　凸版印刷株式会社内

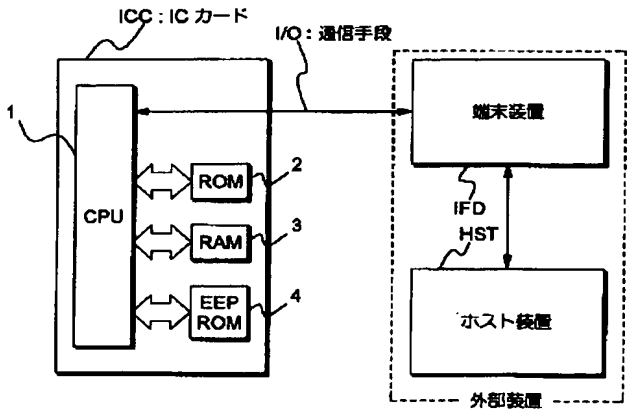
(74)代理人　弁理士　川▲崎▼　研二

(54)【発明の名称】　ＩＣカードおよびＩＣカードシステム

(57)【要約】

【課題】　不正にＩＣカードのデータを入手することを防止するＩＣカードおよびＩＣカードシステムを提供する。

【解決手段】　ＣＰＵ１は、ＥＥＰＲＯＭ４に格納されるデータである付加データに対して、一つの命令データを端末装置ＩＦＤ側から受信する毎に所定値を一方向的に加算又は減算する。さらに、ＣＰＵ１は、その加算又は減算された付加データを前記命令データに付加し、この付加データが付加された命令データを特定の秘密鍵によって暗号化して通信手段上で送受信されるデータとする。



1

【特許請求の範囲】

【請求項１】　外部装置から受信した命令データに従って所定の処理を行うＩＣカードにおいて、
前記命令データを認証するための認証データを記憶する認証データ記憶手段と、
前記認証データを、前記受信に先だって前記外部装置に送信する認証データ送信手段と、
前記認証データと前記命令データとに基づいて生成された認証付命令データを受信すると、当該認証付命令データ中の認証データと、前記認証データ記憶手段に記憶された認証データとを比較し、当該比較結果に基づいて、前記命令データが正当なデータであるか否かを判定する判定手段とを具備することを特徴とするＩＣカード。

【請求項２】　前記認証付命令データは、前記認証データを付加した前記命令データを暗号化して生成されており、
前記判定手段は、前記認証付命令データを復号化することによって、当該認証付命令データ中の認証データと、前記認証データ記憶手段に記憶された認証データとを比較することを特徴とする請求項１に記載のＩＣカード。

【請求項３】　前記認証付命令データは、前記認証データを付加した前記命令データを暗号化した暗号化認証データと前記命令データとを含んで生成されており、
前記判定手段は、前記認証データ記憶手段に記憶された認証データを付加した前記認証付命令データ中の前記前記命令データを暗号化して比較データを生成し、当該比較データと前記暗号化認証データとを比較することによって、当該認証付命令データ中の認証データと、前記認証データ記憶手段に記憶された認証データとを比較することを特徴とする請求項１に記載のＩＣカード。

【請求項４】　当該外部装置から前記認証付命令データを受信する毎に、前記認証データ記憶手段に記憶された認証データを更新する認証制御手段をさらに具備することを特徴とする請求項１ないし３いずれかに記載のＩＣカード。

【請求項５】　前記判定手段は、前記認証付命令データ中の認証データと、前記認証データ記憶手段に記憶された認証データとの差が所定の範囲内であれば、前記命令データが正当なデータであると判定し、
前記認証制御手段は、前記認証データに所定の演算を行うことによって前記更新を行うことを特徴とする請求項４に記載のＩＣカード。

【請求項６】　外部装置と、当該外部装置から受信した命令データに従って所定の処理を行うＩＣカードとを具備するＩＣカードシステムにおいて、
前記ＩＣカードは前記命令データを認証するための認証データを記憶する認証データ記憶手段と、
前記認証データを、前記受信に先だって前記外部装置に送信する認証データ送信手段とを具備し、
前記外部装置は、

2

受信した前記認証データと前記命令データとに基づいて認証付命令データを生成する認証付命令データを生成手段と、
前記認証付命令データを前記ＩＣカードに送信する認証付命令データ送信手段を具備し、
前記ＩＣカードは、
前記認証付命令データを受信すると、当該認証付命令データ中の認証データと、前記認証データ記憶手段に記憶された認証データとを比較し、当該比較結果に基づいて、前記命令データが正当なデータであるか否かを判定する判定手段とを具備することを特徴とするＩＣカードシステム。

【請求項７】　前記認証付命令データ生成手段は、前記認証データを付加した前記命令データを暗号化して前記認証付命令データを生成し、
前記判定手段は、前記認証付命令データを復号化することによって、当該認証付命令データ中の認証データと、前記認証データ記憶手段に記憶された認証データとを比較することを特徴とする請求項６に記載のＩＣカードシステム。

【請求項８】　前記認証付命令データ生成手段は、前記認証データを付加した前記命令データを暗号化した暗号化認証データと前記命令データとを含んだ前記認証付命令データを生成し、
前記判定手段は、前記認証データ記憶手段に記憶された認証データを付加した前記認証付命令データ中の前記前記命令データを暗号化して比較データを生成し、当該比較データと前記暗号化認証データとを比較することによって、当該認証付命令データ中の認証データと、前記認証データ記憶手段に記憶された認証データとを比較することを特徴とする請求項６に記載のＩＣカードシステム。

【請求項９】　当該外部装置から前記認証付命令データを受信する毎に、前記認証データ記憶手段に記憶された認証データを更新する認証制御手段をさらに具備することを特徴とする請求項６ないし８いずれかに記載のＩＣカードシステム。

【請求項１０】　前記判定手段は、前記認証付命令データ中の認証データと、前記認証データ記憶手段に記憶された認証データとの差が所定の範囲内であれば、前記命令データが正当なデータであると判定し、
前記認証制御手段は、前記認証データに所定の演算を行うことによって前記更新を行うことを特徴とする請求項９に記載のＩＣカードシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、データを利用者が物理的に持ち運びできるシステムであるＩＣカードに代表される可搬型データ担保システムに係り、特に、不正にデータが入手されることを防止するのに好適なＩＣ

カードおよびＩＣカードシステムに関する。

【０００２】

【従来の技術】従来のＩＣカードは、ＩＣカードに内蔵されている記憶手段に格納されているデータへの読み書きを、各ファイル毎に複数のパスワードを組み合わせたアクセス権を用いて管理し、データのセキュリティを保っている。なお、通常、ＩＣカードでは、記憶手段内にデータを格納する場合にファイルという概念を適用している。

【０００３】また、前述のアクセス権とは、ファイル毎に設定されているものであり、通常、データの読み出しに関するアクセス権、データの書き換えに関するアクセス権等、ファイルに対する命令の種類毎に複数種類設定できるものである。ＩＣカード内には、そのアクセス権の種類に対応する数のパスワードデータが格納されており、アクセス権の許可は、各ファイル毎に規定されたアクセス権に対応したパスワードを照合することで行っている。つまり正当な権原者とは、ＩＣカード内に格納されたパスワードデータを知り得る者である。

【０００４】例えば、正当権原者によるデータの読み出しには、図２に示すフローチャートのように、まず、当該ファイルに設定されている読み出し命令に対応するアクセス権を満足させるために、パスワード照合コマンドにパスワードデータである秘密鍵データを付加してＩＣカードに送信する（Ｓ１１）。そして、ＩＣカードはその受信した秘密鍵データがＩＣカード内に格納されているものと同一か否かを比較照合する（Ｓ１２）。

【０００５】ここで、受信した秘密鍵データがＩＣカード内に格納されているものと同一であれば、アクセス権を当該読み出し命令に与えるべく、当該秘密鍵の照合状態を照合済みに設定し（Ｓ１３）、照合が成功した旨を返答データとして端末側に送信する（Ｓ１４）。その後、送信されてくる正当な当該ファイルに対するデータ読み出し命令に対し（Ｓ１５）、指定されたアロケーションのデータを返信データとして送信する（Ｓ１６）。

【０００６】一方、ステップ１２において、受信した秘密鍵データがＩＣカード内に格納されているものと同一でない場合は、当該秘密鍵の照合状態を未照合に変更し（Ｓ１７）、変数である連続間違え回数に１を加算する（Ｓ１８）。そして、その加算した連続間違え回数と事前に規定している連続間違え許容回数とを照らし合わせ（Ｓ１９、Ｓ２０）、当該連続間違え回数が連続間違え許容回数と一致した場合、若しくは当該連続間違え回数が連続間違え許容回数よりも大きくなった場合は、当該秘密鍵データが格納されているファイルを閉鎖状態とする（Ｓ２１）。そして、照合が失敗した旨を返答データとして端末側に送信する（Ｓ２２）。

【０００７】

【発明が解決しようとする課題】ところで、正当権利者が前述の図２に示す手順にしたがってパスワードの照合を終了し、当該ファイルに対する読み出し権を獲得した後に、不正アクセス者がＩＣカードの通信手段に侵入して、正当アクセス者が送信したデータを不正アクセス者が複製等することで正当な読み出し命令をＩＣカードに対し送信した場合は、当該ＩＣカードは不正アクセス者に対して前記返信データを返信してしまうという事態が考えられる。このことは、現状のＩＣカードでは防ぎようのないセキュリティ上の抜け道であった。

【０００８】本発明は係る事情に鑑みてなされたものであり、正当アクセス者が送信したデータを不正アクセス者が複製して送信することで、不正にＩＣカードのデータを入手することを防止するＩＣカードおよびＩＣカードシステムを提供することを目的とする。

【０００９】

【課題を解決するための手段】上述した課題を解決するために請求項１記載の発明は、外部装置から受信した命令データに従って所定の処理を行うＩＣカードにおいて、前記命令データを認証するための認証データを記憶する認証データ記憶手段と、前記認証データを、前記受信に先だって前記外部装置に送信する認証データ送信手段と、前記認証データと前記命令データとに基づいて生成された認証付命令データを受信すると、当該認証付命令データ中の認証データと、前記認証データ記憶手段に記憶された認証データとを比較し、当該比較結果に基づいて、前記命令データが正当なデータであるか否かを判定する判定手段とを具備することを特徴とする。

【００１０】また、請求項２に記載の発明は、請求項１に記載の発明において、前記認証付命令データは、前記認証データを付加した前記命令データを暗号化して生成されており、前記判定手段は、前記認証付命令データを復号化することによって、当該認証付命令データ中の認証データと、前記認証データ記憶手段に記憶された認証データとを比較することを特徴とする。

【００１１】また、請求項３に記載の発明は、請求項１に記載の発明において、前記認証付命令データは、前記認証データを付加した前記命令データを暗号化した暗号化認証データと前記命令データとを含んで生成されており、前記判定手段は、前記認証データ記憶手段に記憶された認証データを付加した前記認証付命令データ中の前記前記命令データを暗号化して比較データを生成し、当該比較データと前記暗号化認証データとを比較することによって、当該認証付命令データ中の認証データと、前記認証データ記憶手段に記憶された認証データとを比較することを特徴とする。

【００１２】また、請求項４に記載の発明は、請求項１にないし３いずれかに記載の発明において、当該外部装置から前記認証付命令データを受信する毎に、前記認証データ記憶手段に記憶された認証データを更新する認証制御手段をさらに具備することを特徴とする。

【００１３】また、請求項５に記載の発明は、請求項４

に記載の発明において、前記判定手段は、前記認証付命令データ中の認証データと、前記認証データ記憶手段に記憶された認証データとの差が所定の範囲内であれば、前記命令データが正当なデータであると判定し、前記認証制御手段は、前記認証データに所定の演算を行うことによって前記更新を行うことを特徴とする。

【００１４】また、請求項６に記載の発明は、外部装置と、当該外部装置から受信した命令データに従って所定の処理を行うＩＣカードとを具備するＩＣカードシステムにおいて、前記ＩＣカードは前記命令データを認証するための認証データを記憶する認証データ記憶手段と、前記認証データを、前記受信に先だって前記外部装置に送信する認証データ送信手段とを具備し、前記外部装置は、受信した前記認証データと前記命令データとに基づいて認証付命令データを生成する認証付命令データを生成手段と、前記認証付命令データを前記ＩＣカードに送信する認証付命令データ送信手段を具備し、前記ＩＣカードは、前記認証付命令データを受信すると、当該認証付命令データ中の認証データと、前記認証データ記憶手段に記憶された認証データとを比較し、当該比較結果に基づいて、前記命令データが正当なデータであるか否かを判定する判定手段とを具備することを特徴とする。

【００１５】また、請求項７に記載の発明は、請求項６に記載の発明において、前記認証付命令データ生成手段は、前記認証データを付加した前記命令データを暗号化して前記認証付命令データを生成し、前記判定手段は、前記認証付命令データを復号化することによって、当該認証付命令データ中の認証データと、前記認証データ記憶手段に記憶された認証データとを比較することを特徴とする。

【００１６】また、請求項８に記載の発明は、請求項６に記載の発明において、前記認証付命令データ生成手段は、前記認証データを付加した前記命令データを暗号化した暗号化認証データと前記命令データとを含んだ前記認証付命令データを生成し、前記判定手段は、前記認証データ記憶手段に記憶された認証データを付加した前記認証付命令データ中の前記前記命令データを暗号化して比較データを生成し、当該比較データと前記暗号化認証データとを比較することによって、当該認証付命令データ中の認証データと、前記認証データ記憶手段に記憶された認証データとを比較することを特徴とする。

【００１７】また、請求項９に記載の発明は、請求項６ないし８いずれかに記載の発明において、当該外部装置から前記認証付命令データを受信する毎に、前記認証データ記憶手段に記憶された認証データを更新する認証制御手段をさらに具備することを特徴とする。

【００１８】また、請求項１０に記載の発明は、請求項９に記載の発明において、前記判定手段は、前記認証付命令データ中の認証データと、前記認証データ記憶手段に記憶された認証データとの差が所定の範囲内であれば、前記命令データが正当なデータであると判定し、前記認証制御手段は、前記認証データに所定の演算を行うことによって前記更新を行うことを特徴とする。

【００１９】

【発明の実施の形態】以下、図面を参照して、この発明の実施形態を説明する。

Ａ：実施形態の構成

【００２０】図１は、本発明の１の実施形態であるＩＣカードシステムの構成を示すブロック図である。図示するように、本発明にかかるＩＣカードＩＣＣは、外部装置と通信手段Ｉ／Ｏを介して通信可能に接続でき、外部装置は、ＩＣカードＩＣＣに対してアクセスを行うための装置である端末装置ＩＦＤと、端末装置ＩＦＤと接続されたホスト装置ＨＳＴとを備えている。

【００２１】ＩＣカードＩＣＣは、ＣＰＵ１、ＲＯＭ２、ＲＡＭ３、およびＥＥＰＲＯＭ４を備えている。ＣＰＵ１は、ＲＯＭ２に格納されている当該ＩＣカードのオペレーティングシステムであるカードＯＳのプログラムに従って、各種処理を制御する。ＲＡＭ３は、入出力データ及びプログラム実行時のデータ等の一時待避等に使用され、ＥＥＰＲＯＭ４は、不揮発的にデータを保持するとともに書き換え可能にデータを保持する不揮発性データ記憶手段となる。

【００２２】端末装置ＩＦＤは、例えばＩＣカード専用のリーダライタであり、ホスト装置ＨＳＴは、端末装置ＩＦＤにおける動作の制御等を行うものである。また、通信手段Ｉ／Ｏは、ＩＣカードＩＣＣと端末ＩＦＤとの間で、コマンドやデータを送受信するためのものである。

【００２３】Ｂ：実施形態の動作

次に、上記構成からなるＩＣカードシステムの動作を説明する。図３は、本ＩＣカードシステムの動作を示すフローチャートである。また、図４は、端末装置ＩＦＤにおける暗号化の方法を示す図であり、図５は、ＩＣカードＩＣＣにおける復号化の方法を示す図である。まず、ＣＰＵ１は、ＩＣカードＩＣＣに対しての端末装置ＩＦＤ側から送信された「付加データ」通知コマンドを受け、不揮発性データ記憶手段であるＥＥＰＲＯＭ４に格納されている「付加データ」の値を端末装置ＩＦＤ側にレスポンスとして通知する（Ｓ３１）。なお、「付加データ」通知コマンドは、正当権利者のみが知り得るコマンドである。

【００２４】次に、この「付加データ」を受信した端末装置ＩＦＤ側は、図４に示すように、ＩＣカードにコマンドを発行するために、コマンドのＡＰＤＵ（ApplicationProtocol Data Unit）部の最終バイトに当該「付加データＮｎ」を付加し、このデータを秘密鍵によって暗号化して、コマンドとしてＩＣカードに送信する（Ｓ３２）。ＣＰＵ１は、図５に示すように、受信したコマンドデータを秘密鍵によって複合化し（Ｓ３３）、平文の

コマンドデータと最終データに付加された「付加データＮｎ」とを取り出す（Ｓ３４）。ＣＰＵ１は、この取り出した「付加データＮｎ」とＥＥＰＲＯＭ４に格納されている「付加データ」とを比較し（Ｓ３５）、同一であれば正当権原者からのコマンドであると判断する。

【００２５】ここで、ＣＰＵ１は、正当権原者からのコマンドと判断した場合は、その比較した「付加データ」に１を加算して新しい「付加データ」とし、この新しい「付加データ」をＥＥＰＲＯＭ４に格納する（Ｓ３６）。そして、復号化処理によって得られた当該コマンドを実行する処理を行い（Ｓ３７）、その処理結果をレスポンスデータとして端末装置ＩＦＤ側に送信する（Ｓ３８）。

【００２６】また、ステップ３５において、正当権原者であると判断できなかった場合は、ＣＰＵ１は、その旨をレスポンスデータとして端末装置ＩＦＤ側に通知する。このように、ＣＰＵ１は、ＥＥＰＲＯＭ４に格納されている付加データに対して、端末装置ＩＦＤ側から一つの命令データを受信する毎に、１を加算する。そして、当該加算後の付加データを新しい「付加データ」として当該命令データに付加する。さらに、ＣＰＵ１は、付加データが付加された命令データを特定の秘密鍵によって暗号化して通信手段で送受信されるデータとする。

【００２７】これらにより、ＩＣカードＩＣＣは、不正アクセス者がＩＣカードＩＣＣの通信手段に侵入し、正当アクセス者が事前に送信した命令データを当該不正アクセス者が複製して正当な読み出し命令をＩＣカードに対し送信した時でも、この時はすでに付加データを変更しているので、当該不正アクセス者に対して返信データを返信してしまうことを防止することができる。

【００２８】Ｃ：変形例

本変形例は、本発明の第２の実施形態であり、図１に示す第１実施形態のＩＣカードシステムと同じ構成を有するとともに、以下に述べる機能をも有するものである。図６は、本実施形態のＩＣカードシステムの動作を示すフローチャートである。また、図７は、端末装置ＩＦＤにおける暗号化の方法を示す図であり、図８はＩＣカードＩＣＣにおける復号化の方法を示す図である。

【００２９】まず、ＣＰＵ１は、ＩＣカードＩＣＣに対しての端末装置ＩＦＤ側から送信された「付加データ」通知コマンドを受け、不揮発性データ記憶手段であるＥＥＰＲＯＭ４に格納されている「付加データ」の値を端末装置ＩＦＤ側にレスポンスとして通知する（Ｓ６１）。次に、この「付加データ」を知り得た端末装置ＩＦＤ側は、ＩＣカードにコマンドを発行するために、図７に示すように、コマンドのＡＰＤＵ部の最終バイトに当該「付加データＮｎ」を付加し、このデータを秘密鍵によってＣＢＣ（Cipher Block Chainning）モードにより暗号化し、認証子生成検査法によるコードであるＭＡＣ（Massage Authentication Cord）を生成し、このＭＡＣに平文のコマンドを付加してＩＣカードに送信する（Ｓ６２）。

【００３０】ＣＰＵ１は、図８に示すように、ＥＥＰＲＯＭ４に格納されている「付加データ」を受信したコマンドデータのＡＰＤＵ部に付加し、これを秘密鍵によってＣＢＣモードで暗号化してＭＡＣ’を生成する（Ｓ６３）。そして、ＣＰＵ１は、受信したコマンドに付加されたＭＡＣと自らが生成したＭＡＣ’とを比較し（Ｓ６４）、同一であれば正当権原者からのコマンドであると判断する。

【００３１】ここで、ＣＰＵ１は、正当権原者からのコマンドと判断した場合は、「付加データ」に１を加算して新しい「付加データ」とし、この新しい「付加データ」をＥＥＰＲＯＭ４に格納する（Ｓ６５）。そして、ＣＰＵ１は、受信した当該コマンドを実行する処理を行い（Ｓ６６）、その処理結果をレスポンスデータとして端末装置ＩＦＤ側に送信する（Ｓ６７）。また、ステップ６４において、正当権原者であると判断できなかった場合は、ＣＰＵ１は、その旨をレスポンスデータとして端末装置ＩＦＤ側に通知する。

【００３２】これらにより、ＩＣカードＩＣＣは、付加データの値を、所定の命令に対する返答データの一部として端末側に通知するので、端末装置ＩＦＤ側が他の端末装置に変更された場合でも当該所定の命令を送信する端末装置のみ正当権原者と判断することができる。そして、ＩＣカードＩＣＣは、正当権原者がＭＡＣの照合を終了して、当該コマンドに対する読み出し及び書き込み権を獲得した後に、不正権原者がＩＣカードＩＣＣの通信手段Ｉ／Ｏに侵入し、正当権原者が事前に送信した命令データを当該不正アクセス者が複製して正当な読み出し命令をＩＣカードＩＣＣに対し送信した時でも、この時はすでに付加データが変更されているので、当該不正権原者に対して返信データを返信してしまうことを防止することができる。

【００３３】上記実施形態においては、付加データの値を、所定の命令に対する返答データを用いて端末装置ＩＦＤ側に通知するが、本発明はこれに限定されるものではなく、付加データの値を、各ＩＣカードＩＣＣの属性を示すデータである初期応答データ内に含めることで、当該付加データの値を端末側に通知してもよい。

【００３４】また、上記実施形態においては、ＣＰＵ１は正当権原者からのコマンドと判断した毎に付加データに１を加算しているが、本発明はこれに限定されるものではなく、正当権原者からのコマンドと判断した毎に付加データから所定値を減算又は、加算するものでもよい。

【００３５】また、加算又は減算に限らず、例えば、乗算や除算あるいは複雑な数式といった演算方法を用いても良い。このような場合は、コマンドに付された「付加データ」とＩＣカードＩＣＣに記憶されている「付加デ

ータ」の数値が、同一または所定の差の範囲であれば、両者は一致するものとしてコマンドを送信した者が正当権原者であると判定するようにしてもよい。要は、「付加データ」が、外部装置から受信したコマンドが正当な受信データであることを認証するための認証データとなればよい。

【００３６】

【発明の効果】以上説明したように、この発明によれば、ＩＣカード内に不揮発的に保持される付加データに対して、一つの命令データを受信する毎に、付加データに所定値を一方向的に加算又は減算して新たな付加データとし、この付加データを前記命令データに付加し、この付加データが付加された命令データを暗号化して前記通信手段上で送受信されるデータとするので、同じ内容のコマンドをＩＣカード側に送る場合でも、そのコマンドを送る毎に毎回異なるデータが必要となる。これにより、この発明によれば、端末側とＩＣカード側とでコマンド／レスポンスのやりとりをする際に、ＩＣカードのセキュリティの根本である正当性認証が終了した後に、不正権原者が通信回線に不正に割り込み、正当権原者が送信したコマンドと同一のコマンドを送信することによって、不正権原者がＩＣカードとの間でコマンド／レス＊ポンスのやりとりをすることを防止できるＩＣカードおよびＩＣカードシステムを提供することができる。

＊

【図面の簡単な説明】

【図１】　本発明の第１実施形態であるＩＣカードシステムの構成を示すブロック図である。

【図２】　従来のＩＣカードの構成を示すフローチャートである。

【図３】　本発明の第１実施形態であるＩＣカードの動作を示すフローチャートである。

【図４】　図３に示すＩＣカードにおける暗号化の方法を示す説明図である。

【図５】　図３に示すＩＣカードにおける暗号化の方法を示す説明図である。

【図６】　本発明の第２実施形態であるＩＣカードの動作を示すフローチャートである。

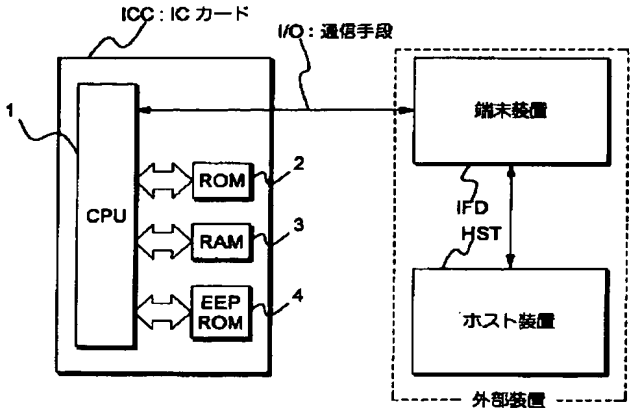
【図７】　図５に示すＩＣカードにおける暗号化の方法を示す説明図である。

【図８】　図５に示すＩＣカードにおける暗号化の方法を示す説明図である。

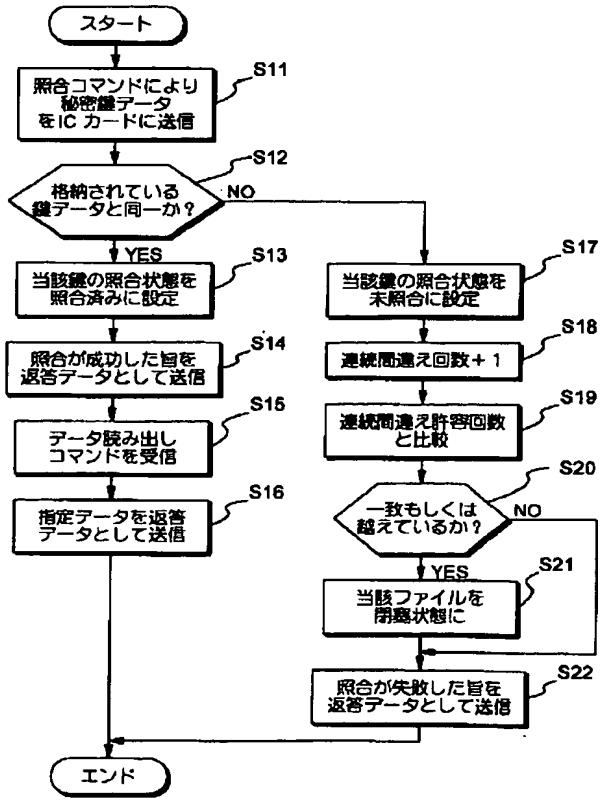
【符号の説明】

１…ＣＰＵ、２…ＲＯＭ、３…ＲＡＭ、４…ＥＥＰＲＯＭ。

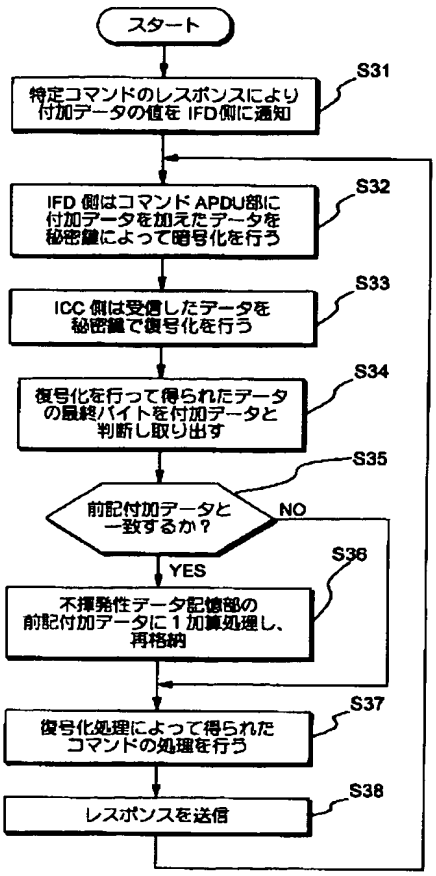
【図１】



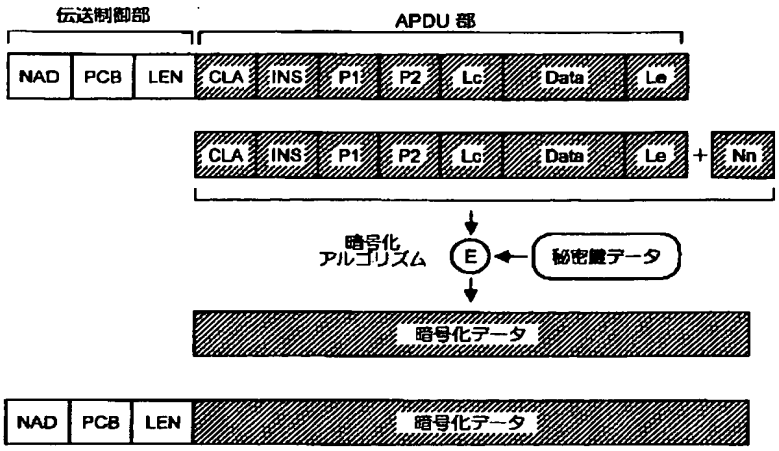
【図２】



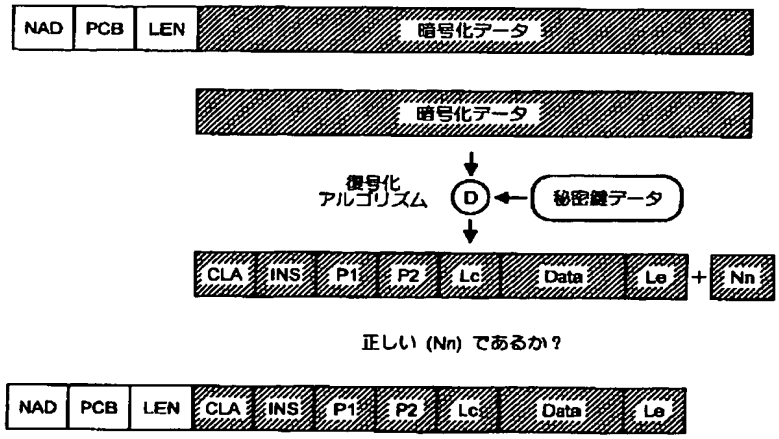
【図３】


スタート
特定コマンドのレスポンスにより付加データの値を IFD側に通知
S31
IFD 側はコマンド APDU部に付加データを加えたデータを秘密鍵によって暗号化を行う
S32
ICC 側は受信したデータを秘密鍵で復号化を行う
S33
復号化を行って得られたデータの最終バイトを付加データと判断し取り出す
S34
前記付加データと一致するか？
S35
NO
YES
不揮発性データ記憶部の前記付加データに１加算処理し、再格納
S36
復号化処理によって得られたコマンドの処理を行う
S37
レスポンスを送信
S38

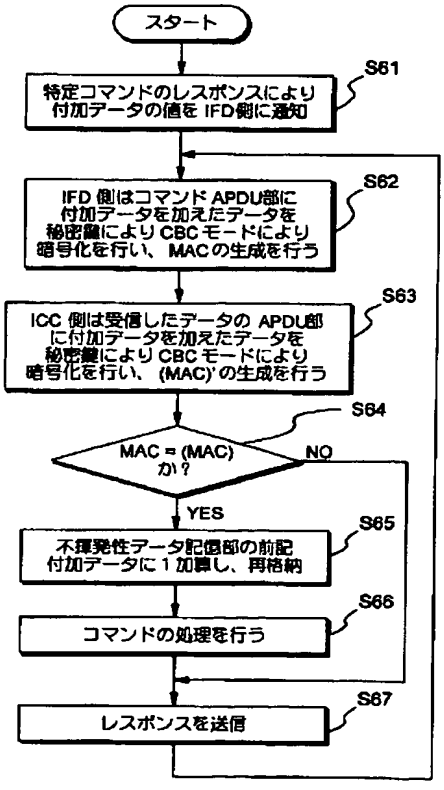
【図４】


伝送制御部
APDU 部
NAD
PCB
LEN
CLA
INS
P1
P2
Lc
Data
Le
Nn
暗号化アルゴリズム
E
秘密鍵データ
暗号化データ

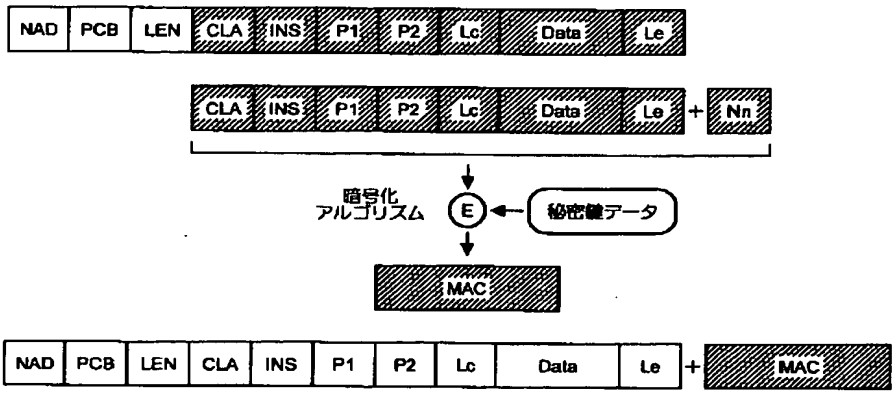
【図５】


NAD
PCB
LEN
暗号化データ
暗号化データ
復号化アルゴリズム
D
秘密鍵データ
CLA
INS
P1
P2
Lc
Data
Le
Nn
正しい (Nn) であるか？
NAD
PCB
LEN
CLA
INS
P1
P2
Lc
Data
Le

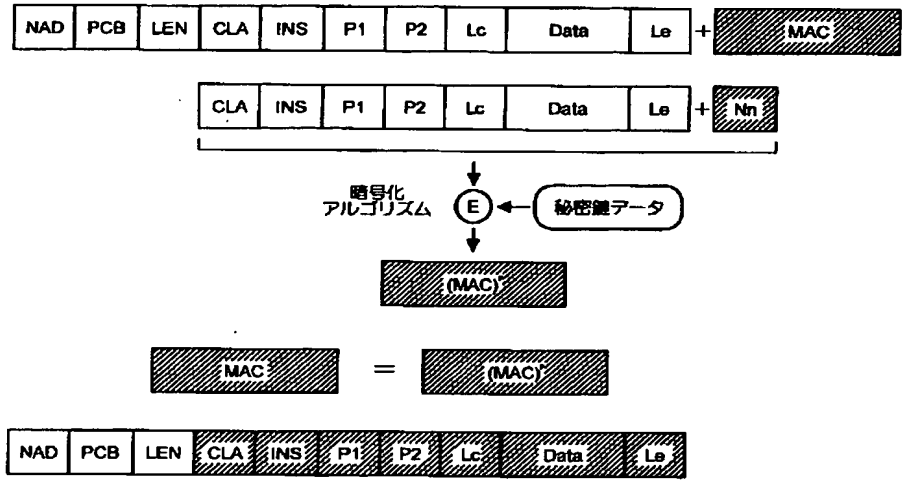
【図６】


スタート
特定コマンドのレスポンスにより付加データの値を IFD側に通知
S61
IFD 側はコマンド APDU部に付加データを加えたデータを秘密鍵により CBC モードにより暗号化を行い、MACの生成を行う
S62
ICC 側は受信したデータの APDU部に付加データを加えたデータを秘密鍵により CBC モードにより暗号化を行い、(MAC)'の生成を行う
S63
MAC = (MAC)' か？
S64
NO
YES
不揮発性データ記憶部の前記付加データに１加算し、再格納
S65
コマンドの処理を行う
S66
レスポンスを送信
S67

【図７】


NAD
PCB
LEN
CLA
INS
P1
P2
Lc
Data
Le
CLA
INS
P1
P2
Lc
Data
Le
+
Nn
暗号化
アルゴリスム
E
秘密鍵データ
MAC
NAD
PCB
LEN
CLA
INS
P1
P2
Lc
Data
Le
+
MAC

【図８】


NAD
PCB
LEN
CLA
INS
P1
P2
Lc
Data
Le
+
MAC
CLA
INS
P1
P2
Lc
Data
Le
+
Nn
暗号化
アルゴリスム
E
秘密鍵データ
(MAC)'
MAC
=
(MAC)'
NAD
PCB
LEN
CLA
INS
P1
P2
Lc
Data
Le